Efficient Numerical Frameworks for Multi-Objective Cyber Security Planning

MHR. Khouzani*, P. Malacaria*, C. Hankin†, A. Fielder†, F. Smeraldi*

Queen Mary University of London*, Imperial College London†

Abstract. We consider the problem of optimal investment in cyber-security by an enterprise. Optimality is measured with respect to the overall (1) monetary cost of implementation, (2) negative side-effects of cyber-security controls (indirect costs), and (3) mitigation of the cyber-security risk. We consider "passive" and "reactive" threats, the former representing the case where attack attempts are independent of the defender's chosen plan, the latter, where attackers can adapt and react to an implemented cyber-security defense. Moreover, we model in three different ways the combined effect of multiple cyber-security controls, depending on their degree of complementarity and correlation. We also consider multi-stage attacks and address the potential correlations in the success of different stages. First, we formalize the problem as a non-linear multi-objective integer programming. We then convert these optimizations into Mixed Linear Integer Programs (MILP) that very efficiently solve for the exact Pareto-optimal solutions even when the number of available controls is large. In our numerical evaluation section, we perform the largest cyber-security modeling to date: our case study comprises 27 of the most typical security controls, each with multiple intensity levels of implementation, and 37 common vulnerabilities facing a typical SME. We compare our findings against expert-recommended critical controls. We then investigate the effect of the security models on the resulting optimal plan and contrast the merits of different security metrics. In particular, we show the superior robustness of the security measures based on the "reactive" threat model, and the significance of the hitherto overlooked role of correlations.

1 Introduction

A cyber-security plan is a set of defensive measures (i.e., cyber-security controls) that are applied across an enterprise to improve its overall state of security. There are many cyber-security measures to choose from, and each measure can be implemented at multiple levels of intensity. Examples of these security controls (taken from the UK's Center for the Protection of National Infrastructure (CPNI)'s list of top-20 critical measures [22]) include: "Inventory of Authorized and Unauthorized Devices", "Inventory of Authorized and Unauthorized Software", "Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers", "Malware Defenses", "Wireless Access Control", and so on. Each cyber-security measure addresses a specific set

of vulnerabilities. For instance, while "Access Control" can mitigate "OS Command Injection", it has no effect on "DDoS attacks". Hence a cyber-security plan should be composed of a combination of the measures to provide a well-rounded defense against the range of vulnerabilities that the enterprise faces.

Implementation of each cyber-security measure is not cost-free: it requires monetary investment (direct costs) and can also negatively affect the performance of an enterprise (indirect costs). Therefore, an exhaustive implementation of controls at maximum intensity is likely neither economically feasible nor managerially desirable. In reality, organizations have to deal with cyber-security risk within a limited budget and must be wary of the potential side-effects of the security measures on their existing business processes. Therefore, the mitigation in the security risks has to be judiciously balanced with the direct and indirect costs. A selection analysis should consider the set of controls as well as vulnerabilities jointly. This is because an approach that takes investment decisions for each vulnerability or control separately, ignores the relative importance of the vulnerabilities, and does not optimally use the complementary effects of the controls, and hence, may fail to reach a best overall trade-off. Choosing a desirability metric for a plan is itself a challenging task:

1. The three sources of costs (security, direct and indirect) are not easily combinable. For instance, the investment costs are incurred deterministically and at the present, while the security losses are probabilistic in nature and, if at all, will occur at an unknown future time. Also the monetary conversion is not as clear for indirect costs as for the other two, for instance, it is hard to put a monetary value on the annoyance felt by the staff as a result of a more restrictive access control or a stricter password policy.
2. The trade-off preferences cannot be exactly arbitrated "a priori". For instance, even a "security-concerned" enterprise may choose a different plan if "almost" the same security risk mitigation can be achieved at a much lower direct or indirect cost. Likewise, an enterprise that is very sensitive to indirect costs or extra investment may reconsider if a slight increase in these costs can reduce a relatively significant amount of security risk.

To address these issues we adopt a multi-objective optimization framework. Specifically, we simultaneously minimize the security risk, indirect, and direct costs of the enterprise (the latter within the budget). The "solution" of this three-objective optimization is the set of Pareto-optimal (or non-inferior, or simply, Pareto) plans, that are the solutions with the guarantee that no other plan can simultaneously improve all of these three costs (at least one of them strictly).

Of these three costs, the security risk is the most challenging to model. The effect of an individual security measure (at each implementation intensity) can be represented by its "effectiveness" against different vulnerabilities. That is, the reduction in the success probability of exploitation attempts of each vulnerability when only that control is implemented (stand-alone). Complicating the matter is the fact that, often, the same vulnerability can be (partially) mitigated by more than one security measure. Then a modeling question is how to capture the combined efficacy of controls on their overlapping vulnerabilities.

The simplest approach is an "additive" model, where it is assumed that, per each vulnerability, the (blocking) efficacies of controls are added up, heeding that, logically, none of the overall blocking probabilities should exceed 100%. This capping of the combined efficacies introduces a degree of nonlinearity in the model, but one that can be easily dealt with, as we will show later.

Although computationally the simplest, this model bears the underlying assumption that defensive mechanisms have positive externalities on each others' efficacies. In particular, it potentially allows 100% efficacy when multiple controls are combined, which is rather unrealistic. A more relaxed modeling assumption is that each control affects the common vulnerabilities independently. Hence, when a vulnerability is attempted, the success chance is the product of successfully bypassing each of its pertaining controls. We will thus refer to this model as "multiplicative". This model is ostensibly nonlinear in the decision variables, and hence, solving the resulting nonlinear integer program accurately can be very inefficient. However, as we will see later, it can be converted into a Mixed Integer Linear Program (MILP) which is much more efficient to solve accurately.

A problem with the previous two models is that they ignore the possible correlations in the defensive mechanisms of security measures. Due to such correlations, it can be argued that if an attempted exploitation bypasses one of the controls, it will be a strong indication for bypassing the other affecting measures as well. The "independent" blocking probabilities in the heart of multiplicative model, although better than the additive model, can still be a significant over-estimation of the overall effectiveness of a security plan. In this paper, we introduce a novel non-linear model, which we call "best-of", that captures such correlations. In particular, the combined effectiveness of implemented controls on a common vulnerability is taken to be (only) the highest effectiveness among them. We then develop a technique to convert the resulting nonlinear integer program into a MILP that is surprisingly efficient to solve.

Another challenge in modeling the security losses is anticipating the distribution of exploitation attempts of the attackers across vulnerabilities. One approach is to use the histogram of the past attempts (retrieved from the logs of the enterprise itself or of any similar enterprises), or the publicly available statistics of attacks (e.g. [14]). We will refer to this model as the "passive" threat. However, in reality the distribution of the attempts may adapt to the implementation of security controls: if a vulnerability is now well mitigated, then the attempts may shift to other less protected vulnerabilities. We will refer to this case as "Reactive" threat, and establish a connection with a sequential game between the enterprise and attackers. For both passive and reactive cases, we provide efficient ways to solve for the exact Pareto-optimal plans efficiently by converting the nonlinear optimization problems into appropriate MILPs.

Finally, we will present a case study and numerical evaluations using our frameworks and a database of major security controls and vulnerabilities. We first compare the derived optimal plans of each model against the expert recommended list of critical controls, which reveals a general consistency, with best match observed for the "best-of – reactive" model. Subsequently, we compare the optimal plans as well as the achieved utilities across our different security

risk models. In particular, we observe that the "reactive" threat provides a more robust (and hence more favorable) notion of security risk in the sense that, optimization with respect to reactive threat does not lead to a terribly sub-optimal performance with respect to passive threat, however, the opposite is not true: an optimal plan with respect to passive threat can lead to terrible performance with respect to reactive threat, even for relatively high values of investment budget.

Contributions and Related Works

There are two main contributions of this work:

- By reducing the model to MILP we make possible to compute optimal solutions for cyber-security: the state space we consider in our case study is enormous, of the order of 10^{14} pure strategies, and our MILP finds the optimal solution in seconds. The closest work in the cyber-security literature [24] takes instead days to converge and crucially lacks a guarantee of optimality.
- Our case study represents the largest cyber-security modeling to date. The data used in the experiments has been extracted from official government organizations' publications like [4, 5, 17] as well as the publicly available databases of CVE, CWE and CWSS.

Quantitative risk assessment and mitigation in cyber-security has been a thematic topic of research in security, that has in part lead to established methodologies such as Magerit and NIST800-30 among others [21]. Works that explicitly investigate the problem of investment portfolios in cyber-security include [1–3, 7, 8, 11–13, 15, 16, 18–20, 24]. Comparing with all these work, our work presents a wider modeling framework both in terms of the way controls can be combined (multiplicative, additive, best-of) and in terms of the attacker capabilities and threat types (passive, reactive, cost-based). Also of the above works only [13,16,24] are based on real world data and only [13,24] model indirect costs. Compared with these last two works their solutions are based on Tabu Search (TS) and genetic algorithms (GA) respectively, and are inherently more inefficient than the solutions here presented and they do not provide any guarantee of optimality. Also none of those works addresses issues like robustness.

2 Modeling and Notations

Let $\mathcal{C}$ represent the set of (cyber-security) *controls*, each with potentially multiple intensity levels of implementation. We will use $\mathcal{L}_c = \{1, \ldots, L_c\}$ to denote the set of available implementation levels of control c. A *cyber-security plan* or a cyber-security investment portfolio $\boldsymbol{x} = (x_c)$ is a vector in $\mathcal{X} := \times_{c \in \mathcal{C}}(\{0\} \cup \mathcal{L}_c)$, where $x_c = l \in \{0\} \cup \mathcal{L}_c$ represents the decision to implement control c at level l, with zero representing the lack of implementation of that control.

Let $B \in \mathbb{R}^+$ be the (hard) constraint on the total cyber-security *budget* of the enterprise. Let $D, I, R : \mathcal{X} \to \mathbb{R}^+$ respectively denote the (total) *direct cost*, (total) *indirect cost*, and the (aggregate) *"security risk"* of the enterprise given a security plan. As we proceed, we explicitly describe each of these functions. But

first, we give a high-level description of the problem of cyber-security investment as a (constrained) multi-objective integer programming:

$$\min_{\boldsymbol{x}\in\mathcal{X}} \left(D(\boldsymbol{x}), I(\boldsymbol{x}), R(\boldsymbol{x})\right) \qquad \text{s.t.:} \;\; D(\boldsymbol{x}) \leq B \tag{1}$$

For each $c \in \mathcal{C}$, let $d_c(l) \in \mathbb{R}^+$ be the direct cost of implementing control c at level $l \in \{0\} \cup \mathcal{L}_c$, with the obvious convention that $d_c(0) = 0$. The direct cost is a combination of the (one-time) investment (for obtaining the required hardware, software or staff), and the recurrent monetary expenses associated with the implementation. For controls that are already in place, i.e., existing controls, only the recurrent expenses must be considered. Similarly, let $i_c(l) \in \mathbb{R}^+$ be the indirect cost of implementing control $c \in \mathcal{C}$ at level $l \in \{0\} \cup \mathcal{L}_c$, where $i_c(0) = 0$. The indirect costs are those related to reduced performance (due to introduced overhead on resources), lowered morale (e.g. due to restricting access, false positives, stricter password policies), etc, that are not easily convertible to monetary losses. Using these notations, we simply have:

$$D(\boldsymbol{x}) = \sum_{c\in\mathcal{C}} d_c(x_c), \qquad I(\boldsymbol{x}) = \sum_{c\in\mathcal{C}} i_c(x_c) \tag{2}$$

We will denote the set of vulnerabilities of the enterprise by $\mathcal{V}$. Let $e_{cv}(l)$ be the stand-alone *effectiveness* of control c at implementation level $l \in \{0\} \cup \mathcal{L}_c$ on vulnerability v, that is, $e_{cv}(l)$ is the probability that an exploitation attempts on vulnerability v is blocked when "only" control c at implementation level l is present. Then $s_{cv}(l) := 1 - e_{cv}(l)$ will represent the success probability of an attempt at exploitation of vulnerability v when no other control than c at level l is implemented. Trivially, $e_{cv}(0) = 0 \; \forall c \in \mathcal{C}$ and $\forall v \in \mathcal{V}$.

Let $\mathcal{C}_v$ be the set of controls that can affect vulnerability v, i.e., $\mathcal{C}_v := \{c \in \mathcal{C} : e_{cv}(l) > 0 \text{ for some } l \in \mathcal{L}_c\}$. If for a vulnerability v, we have $\|\mathcal{C}_v\| > 1$, then the combined effectiveness of the controls on v needs to be modeled. In particular, let $S_v : \mathcal{X} \to [0, 1]$ represent the success probability of an exploitation attempt on vulnerability $v \in \mathcal{V}$ given a cyber-security plan. We provide three different candidates for $S_v(\boldsymbol{x})$, in decreasing order of "complementary" effects among the defensive mechanisms of the controls (using the convention: $a^+ := \max\{a, 0\}$):

$$\text{Additive:} \qquad S_v(\boldsymbol{x}) = \big(1 - \sum_{c\in\mathcal{C}_v} e_{cv}(x_c)\big)^+ \tag{3}$$

$$\text{Multiplicative:} \qquad S_v(\boldsymbol{x}) = \prod_{c\in\mathcal{C}_v} s_{cv}(x_c) \tag{4}$$

$$\text{Best-of:} \qquad S_v(\boldsymbol{x}) = \min_{c\in\mathcal{C}_v} s_{cv}(x_c) \tag{5}$$

Let Λ_v be the random variable representing the losses to the enterprise when vulnerability $v \in \mathcal{V}$ is "successfully" exploited, and let λ_v be its expected value. These losses are due to the interruption in availability, integrity and/or confidentiality of data assets or services of the enterprise (e.g. tampering or theft of intellectual property or financial or client data, disruption of operations, *etc.*) as

well as the secondary causes of losses such as reputation damage, loss of clients, legal fees, and so on.[1] We assume a "risk-neutral" decision-maker, and hence take the expected value of losses due to successful exploitations to be the measure of the security risk. In order to represent the expected losses, we need to anticipate the rate with which different vulnerabilities will be target of exploitation. This rate may depend on the profile of the enterprise and may also change in the face of the implemented security plan. Let $\pi : \mathcal{X} \to \Delta(\mathcal{V})$ represent this relation, where $\Delta(\mathcal{V})$ represents the set of all probability distributions over the set of vulnerabilities $\mathcal{V}$. In particular, let $\pi(v; \boldsymbol{x})$ be the rate at which vulnerability $v \in \mathcal{V}$ is attempted, given that the implemented plan is $\boldsymbol{x}$. Then the security risk of the (risk-neutral) enterprise in (1) can be written as:

$$R(\boldsymbol{x}) = \sum_{v \in \mathcal{V}} \pi(v; \boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v \tag{6}$$

Modeling π requires anticipating the behavior of the attackers. In what follows, we consider two models for this behavior: "passive" and "reactive" threats.

Passive Threat In this model, the probability distribution of the attacks is assumed given and that it "stays unchanged" irrespective of the implemented plan. In particular, let $\mathbf{P} \in \Delta\mathcal{V}$ be the distribution of attempts across vulnerabilities, which will be the same for any implemented plan $\boldsymbol{x} \in \mathcal{X}$, i.e., $\pi(v; \boldsymbol{x}) = \mathbf{P}(v)$ $\forall \boldsymbol{x} \in \mathcal{X}$. In the rest of the paper, we will denote $\mathbf{P}(v)$ with P_v for brevity. Then the expected losses (as the risk-neutral measure of security risk) is:

$$R(\boldsymbol{x}) = \sum_{v \in \mathcal{V}} P_v S_v(\boldsymbol{x}) \lambda_v \tag{7}$$

where $S_v(\boldsymbol{x})$ comes from (3), (4) or (5), depending on the combination model.

Reactive Threat As we mentioned, the distribution of attempts for exploiting vulnerabilities may evolve in the face of the new implemented security plan. In particular, the attempts on well-protected vulnerabilities may shift to less protected vulnerabilities. The most pessimistic scenario is the assumption that the attempts will shift to a vulnerability that has the most "effective impact", i.e., in (6): $\sum_{v \in \arg\max(S_v(\boldsymbol{x})\lambda_v)} \pi(v; \boldsymbol{x}) = 1$. Therefore, the corresponding expected loss (as the risk-neutral measure of security risk) is:

$$R(\boldsymbol{x}) = \max_{v \in \mathcal{V}} \left(S_v(\boldsymbol{x}) \lambda_v\right) \tag{8}$$

Next, we show that this notion of security is closely related to a sequential game.

[1] The loss Λ_v is enterprise dependent through their evaluation of different sources of disruption: An energy company may be primarily concerned with the availability of their service while a banking firm would assign a large weight to integrity of its data.

Connection to Game Theory Consider the following non-zero-sum sequential two-player game of "perfect information":

Players: The enterprise 'e' (the leader), and the attacker 'a' (the follower).

Action spaces: The action of the enterprise is its cyber-security investment plan, $\boldsymbol{x}$. The attacker decides on which one of the vulnerabilities to try to exploit (if any). This can be represented by an indicator $\boldsymbol{y}$. Hence, the action spaces are respectively $\mathcal{X}$ and $\mathcal{Y} := \{\boldsymbol{y} \in \{0,1\}^{\mathcal{V}} : \sum_{v\in\mathcal{V}} \boldsymbol{y}(v) \leq 1\}$. The enterprise also has a constraint, defining its set of feasible actions: the total direct cost of its action has to be within the budget, which the attacker may not know the value of.

Information structure & strategies: The enterprise (the leader) makes the first "move", and its action and strategy spaces coincide. The attacker (the follower) observes the "move" of the enterprise $\boldsymbol{x}$ (hence the label: "perfect information"), and after re-assessing the effectiveness of attempts on each of the vulnerabilities, makes its decision of which vulnerability to attempt. Hence, a strategy of the attacker, which we denote by σ, is a function $\sigma : \mathcal{X} \to \mathcal{Y}$, and its strategy space is the set of all functions $\mathcal{X} \to \mathcal{Y}$, denoted by $\mathcal{Y}^{\mathcal{X}}$.

Payoffs The negative payoff of the enterprise (which it wants to minimize) is a weighted sum of the three costs. Specifically, let w_d, w_i, and w_r be the weights of the (total) direct and indirect costs and the security damage to the enterprise, respectively, where $w_d, w_i \geq 0$, and $w_r > 0$. Referring to (2) and (6), the expected cost of the enterprise $u_e : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}^+$ is therefore: $u_e(\boldsymbol{x}, \sigma(\boldsymbol{x})) = w_d \sum_{c\in\mathcal{C}} d_c(x_c) + w_i \sum_{c\in\mathcal{C}} i_c(x_c) + w_r \sum_{v\in\mathcal{V}} \sigma_v(\boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v)$. The payoff of the attacker (which it wants to maximize) is (linearly) proportional to the expected security losses of the enterprise due to successful exploitations. In particular, letting $u_a : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}^+$ represent the expected payoff of the attacker, we can write: $u_a(\boldsymbol{x}, \sigma(\boldsymbol{x})) = w'_r \sum_{v\in\mathcal{V}} \sigma_v(\boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v$, for some $w'_r > 0$, whose exact value may not be known to the enterprise. Note that we assumed exploitation attempts are costless for the attacker. We have the following result:

Prop. 1 *Any strategy of the enterprise in a Subgame Perfect Nash Equilibrium (SPNE) of the above non-zero-sum sequential two player game with "perfect information" is a Pareto-optimal solution to the multi-objective problem of* (1) *where the security cost is according to the "reactive threat" model in* (8).

Proof. Denoting the attacker's best response correspondence by σ^*, we have:

$$\sigma^*(\boldsymbol{x}) \in \arg\max_{v\in\mathcal{V}} w'_r \sum_{v\in\mathcal{V}} \sigma_v(\boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v,$$

which implies $\sum_{v\in\mathcal{V}} \sigma^*_v(\boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v = \max_{v\in\mathcal{V}} (S_v(\boldsymbol{x}) \lambda_v)$. Now, using backward induction (for subgame perfection), the problem of the enterprise becomes:

$$\min_{\boldsymbol{x}\in\mathcal{X}} \left[w_d \sum_{c\in\mathcal{C}} d_c(x_c) + w_i \sum_{c\in\mathcal{C}} i_c(x_c) + w_r \max_{v\in\mathcal{V}} (S_v(\boldsymbol{x}) \lambda_v) \right], \quad \textbf{s.t.} \sum_{c\in\mathcal{C}} d_c(x_c) \leq B.$$

Finally, any solution of the above single optimization is also a Pareto-optimal solution of the multi-objective problem in (8). □

It is worthwhile to note that the set of SPNE stays the same even if the game is converted to a zero-sum game in which the payoff of the attacker (to be maximized) is exactly the same as the total cost of the defender, i.e., if $u_a(\boldsymbol{x}, \sigma(\boldsymbol{x})) = u_e(\boldsymbol{x}, \sigma(\boldsymbol{x})) = w_d \sum_{c\in\mathcal{C}} d_c(x_c) + w_i \sum_{c\in\mathcal{C}} i_c(x_c) + w_r \sum_{v\in\mathcal{V}} \sigma_v(\boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v$. That is, if the attacker wanted to also maximize the investment and indirect costs of the defender, the optimization problem of the enterprise would not change at all. To see this, note that once the enterprise makes its implementation decision, the attacker cannot affect either the direct or indirect costs of the enterprise. Interestingly, this still holds even if the attacker has its own weights on different components of its overall payoff, i.e., if $u_a(\boldsymbol{x}, \sigma(\boldsymbol{x})) = w'_d \sum_{c\in\mathcal{C}} d_c(x_c) + w'_i \sum_{c\in\mathcal{C}} i_c(x_c) + w'_r \sum_{v\in\mathcal{V}} \sigma_v(\boldsymbol{x}) S_v(\boldsymbol{x}) \lambda_v$, for instance, if the attacker emphatically cares about the investment and indirect costs of the enterprise.[2]

Justifiability of Perfect Information Assumption The full observability of the action of the enterprise may be unjustifiable in its literal interpretation. However, the critical point here is the much slower variability of security plans and much faster adaptability of attacks. Specifically, once the security plan is implemented, it will not be modified over a relatively long horizon. Hence, the enterprise can be thought of as having committed to its investment decision. In contrast, the exploitation attempts on different vulnerabilities can explore and "learn" the most effective vulnerability. If the transitory learning phase of the attacker is negligible, then the formalism of perfect information is applicable.

3 Solving the Multi-Objective Optimization

An approach to find the Pareto solutions of multi-objective-optimizations (MOO), including multi-objective integer programs (MOIP) and multi-objective combinatorial optimizations (MOCO) as its sub-branches, is through *scalarization*. Here, we provide a brief overview. The reader may consult the survey papers and textbooks on MOO for more detailed treatment, e.g. [6, 10, 23].

In scalarization methods, the MOO is transformed into (parametric) instances of single-objective optimization problems, the optimal solution of each is also a Pareto-optimal solution of the original MOO problem. The most widely known method is the "linear scalarization", where a weighted sum of the individual objectives constitutes the new objective function to be optimized. Specifically, consider a general n-objective optimization problem of $\min_{\boldsymbol{x}\in\mathcal{X}}(F_i(\boldsymbol{x}))$, $i = 1, \ldots, n$. Then a series of single-objective optimization as the convex combination of (a proper normalization of) each of the objective functions is constructed parameterized by the weight coefficients, that is, $\min_{\boldsymbol{x}\in\mathcal{X}} \sum_{i=1}^{n} w_i \tilde{F}_i(\boldsymbol{x})$, where $w_i > 0$ and $\sum_{i=1}^{n} w_i = 1$, and $\tilde{F}_i$ is a carefully chosen affine transformation

[2] The assumptions that attacks are costless and the reward is linearly proportional to the security damage to the enterprise is important for this observation, and the fact that the attacks for not affect the indirect costs, for instance, through the assumption that if an exploitation attempt fails there is no damage associated with it.

(i.e., normalization) of F_i.[3] Clearly, any solution of the weighted optimization is on the Pareto-front of the original multi-objective problem (because otherwise, there is an alternative solution that simultaneously improves all of the objective functions and at least one of them strictly, which contradicts the optimality in the scalarized problem).[4] The Pareto-optimal solutions are found by "sweeping" the weights over the entire simplex with some granularity, solving each of the single objective optimizations, and storing any "new" solution found.

In our problem, if the weights of the direct, indirect and security costs are respectively $w_d, w_i, w_r \geq 0$, such that $w_d + w_d + w_i = 1$, then, ignoring normalization for brevity, the resulting single objective optimizations (SOO) is:

$$\min_{\boldsymbol{x} \in \mathcal{X}} [w_d D(\boldsymbol{x}) + w_i I(\boldsymbol{x}) + w_r R(\boldsymbol{x})] \qquad \text{s.t.: } D(\boldsymbol{x}) \leq B. \tag{9}$$

The form of $R(\boldsymbol{x})$ in part comes from (7) or (8) depending on the threat model, in which the success rates of each attempted vulnerability comes from (3), (4) or (5) depending on the model for combining efficacies of the controls. Each of these optimizations is an instance of a non-linear integer program, which is NP-hard to solve in general. Exploring the entire set of possible plans can be computationally infeasible since the number of plans is $\prod_{c \in \mathcal{C}} (L_c + 1)$, which grows exponentially in the number of controls (this is for instance, over 10^{14} for our case study in §7). In what follows, we describe a series of tricks that help convert each of these nonlinear integer programs into mixed integer linear programs (MILPs) by introducing carefully designed auxiliary variables. [5]

4 Conversions to (binary) MILP

Common to all of our models is the introduction of binary decision variables as follows: $x_{cl} \in \{0, 1\}$ for each $c \in \mathcal{C}$ and $l \in \mathcal{L}_c$, which represents whether control c is implemented at level $l \in \mathcal{L}_c$. Using this notation, we first enforce that logically at most only one of the implementation levels per each control is selected:

$$\Big(x_{cl} \in \{0, 1\}\ \forall l \in \mathcal{L}_c, \forall c \in \mathcal{C}\Big), \quad \Big(\sum_{l \in \mathcal{L}_c} x_{cl} \leq 1,\ \forall c \in \mathcal{C}\Big). \tag{10}$$

Recall that $\mathcal{L}_c := \{1, \ldots, L_c\}$, and in particular, it did not include level 0. Then the direct and indirect costs can be represented in linear form as follows:

$$D(\boldsymbol{x}) = \sum_{c \in \mathcal{C}} \sum_{l \in \mathcal{L}_c} d_c(l) x_{cl}, \qquad I(\boldsymbol{x}) = \sum_{c \in \mathcal{C}} \sum_{l \in \mathcal{L}_c} i_c(l) x_{cl}. \tag{11}$$

Note that $d_c(l)$ and $i_c(l)$ are now just coefficients of the x_{cl} variables.

[3] The normalization is for numerical efficiency, such that the range of the objective functions becomes comparable, hence increasing the chances that a uniform sweeping of the weights even with a small number of steps finds all the Pareto solutions.

[4] Note, however, that finding all Pareto solutions is not guaranteed in this method.

[5] An alternative scalarization approach is the "epsilon-constraint" method. All of our MILP conversions can be modified for that method in a straightforward manner.

4.1 Additive Model in (3)

For the passive threat, the expected security damage in the additive model is:

$$R(\boldsymbol{x}) = \sum_{v\in\mathcal{V}} P_v\Big(1 - \sum_{c\in\mathcal{C}_v} e_{cv}(x_c)\Big)^+ \lambda_v. \tag{12}$$

In order to get rid of the non-linearity introduced by the "positive part" relation, we introduce auxiliary real-valued[6] variables y_v's for each $v \in \mathcal{V}$ such that: $y_v \geq 0$ and $y_v \geq 1 - \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} e_{cv}(l)x_{cl}$. Note that these two inequalities and the goal of the minimization guarantees that at the solution, we have: $y_v = (1 - \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} e_{cv}(l)x_{cl})^+$, as desired. Therefore, we can replace the security cost with $\sum_{v\in\mathcal{V}} P_v y_v \lambda_v$. Hence, we have the following simple proposition:

Prop. 2 *Each of the scalarized single-objective optimizations in* (9) *for the additive–passive risk model is equivalent to the following MILP:*

$$\min_{(x_{cl},y_v)} \left[w_d \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} + w_i \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} i_c(l)x_{cl} + w_r \sum_{v\in\mathcal{V}} (P_v\lambda_v y_v) \right]$$
$$s.t.:\ (10),\ \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} \leq B,\ \Big(y_v \geq 0,\ y_v \geq 1 - \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} e_{cv}(l)x_{cl} : \forall v \in \mathcal{V}\Big).$$

For the reactive threat, the expected security damage as the security risk is: $R(\boldsymbol{x}) = \max_{v\in\mathcal{V}} \Big\{ \big(1 - \sum_{c\in\mathcal{C}_v} e_{cv}(x_c)\big)^+ \lambda_v \Big\}$. This can be made linear by simply introducing (only) one auxiliary variable z and imposing $z \geq 0$ and $z \geq (1 - \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} e_{cv}(l)x_{cl})\lambda_v$ for "all" $v \in \mathcal{V}$. This yields:

Prop. 3 *Each of the scalarized single objective optimizations in* (9) *for the additive–reactive risk model is equivalent to the following MILP:*

$$\min_{(x_{cl},z)} \Big[w_d \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} + w_i \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} i_c(l)x_{cl} + w_r z \Big]$$
$$s.t.:\ (10),\ \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} \leq B,\ z \geq 0,\ \Big(z \geq \big(1 - \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} e_{cv}(l)x_{cl}\big)\lambda_v\ \forall v \in \mathcal{V}\Big).$$

4.2 Multiplicative model in (4)

For multiplicative model, we provide a modification of the method proposed in [19] and modify it for reactive threats as well. First, we extend the optimization variables x_{cl} to explicitly include level zero for each control as well. Hence the "logical" choice constraint, as opposed to (10), becomes:

$$\Big(x_{cl} \in \{0,1\}\ \forall l \in \mathcal{L}_c \cup \{0\}, \forall c \in \mathcal{C}\Big),\ \Big(\sum_{l\in\mathcal{L}_c\cup\{0\}} x_{cl} = 1,\ \forall c \in \mathcal{C}\Big). \tag{13}$$

[6] hence, "mixed" integer linear program, as opposed to pure integer linear program.

Now, for each vulnerability $v \in \mathcal{V}$, we introduce $\sum_{c\in\mathcal{C}_v}(1+L_c)$ positive real-valued auxiliary ("flow") variables $y_{vcl} \geq 0$, one for each $l \in \mathcal{L}_c \cup \{0\}$ per each control $c \in \mathcal{C}_v$, with the following interpretation: y_{vcl} is the fraction ("flow") of the exploitation attempts on vulnerability v that is "handled" by control c at level l. Let $\mathcal{C}_v$, the set of controls that can affect vulnerability v, be enumerated as follows: $\mathcal{C}_v = \{c_1^v, \ldots, c_{|\mathcal{C}_v|}^v\}$ (the order is immaterial). The total fraction of the exploitation attempts on vulnerability v that is to be handled by the first control in $\mathcal{C}_v$ is 1. That is, for each $v \in \mathcal{V}$, we impose: $\sum_{l\in\mathcal{L}_c\cup\{0\}} y_{vcl} = 1$ where $c = c_1^v$. A portion of these exploitation attempts gets blocked by controls c_1^v, depending on which level it is implemented at, and the "surviving" fraction has to be handled by the next control in $\mathcal{C}_v$. Hence, for each $v \in \mathcal{V}$, we have the following flow-like constraint: $\sum_{l\in\mathcal{L}_c\cup\{0\}} y_{vcl}s_{cv}(l) = \sum_{l\in\mathcal{L}_{c'}\cup\{0\}} y_{vc'l}$, where $c' = c_i^v$ and $c = c_{i-1}^v$ for all $i = 2, \ldots, |\mathcal{C}_v|$. Note that $s_{cv}(l)$ is just a coefficient in this linear equality constraint, and recall the convention that $s_{cv}(0) = 1$ for all $v \in \mathcal{V}$, $c \in \mathcal{C}_v$. The overall probability of success of exploitation attempts of vulnerability v is the fraction that survives the last control in $\mathcal{C}_v$, that is, $\sum_{l\in\mathcal{L}_c\cup\{0\}} y_{vcl}s_{cv}(l)$ where $c = c_{|\mathcal{C}_v|}^v$. Enforcing that only the implemented controls have their blocking effect on the vulnerabilities translates to the following constraint: $y_{vcl} \leq x_{cl}$ $\forall v \in \mathcal{V}$, $\forall c \in \mathcal{C}_v$, $\forall l \in \mathcal{L}_c \cup \{0\}$. This constraint along with (13) ensures that only one level per controls is implemented (including level zero) and only the flow-variable corresponding to the implemented level can be nonzero. Now, recursively putting the equalities together will recover the multiplicative form of the overall success probability of exploitation of v. Putting all ingredients together, we have:

Prop. 4 *Each of the scalarized single objective optimizations in* (9) *for the multiplicative–passive risk model is equivalent to the following MILP:*

$$\min_{(x_{cl},y_{cvl})} \Big[w_d \sum_{c\in\mathcal{C}}\sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} + w_i \sum_{c\in\mathcal{C}}\sum_{l\in\mathcal{L}_c} i_c(l)x_{cl} + w_r \sum_{v\in\mathcal{V}} P_v\lambda_v \sum_{\substack{l\in\mathcal{L}_c\cup\{0\}\\ c=c_{|\mathcal{C}_v|}^v}} y_{vcl}s_{cv}(l)\Big]$$

$$\text{s.t.: } (13),\ \sum_{c\in\mathcal{C}}\sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} \leq B,\ \Big(0 \leq y_{vcl} \leq x_{cl} : \forall v \in \mathcal{V}, \forall c \in \mathcal{C}_v, \forall l \in \mathcal{L}_c \cup \{0\}\Big),$$

$$\Big(\sum_{l\in\mathcal{L}_c\cup\{0\}} y_{vcl} = 1 :\ c = c_1^v,\ \forall v \in \mathcal{V}\Big), \tag{14}$$

$$\sum_{l\in\mathcal{L}_{c'}\cup\{0\}} y_{vc'l} = \sum_{l\in\mathcal{L}_c\cup\{0\}} y_{vcl}s_{cv}(l) : c' = c_i^v, c = c_{i-1}^v, \forall i = 2, \ldots, |\mathcal{C}_v|, \forall v \in \mathcal{V}.$$

For the reactive threat model, we can introduce an extra variable z and enforce: $z \geq \lambda_v \sum_{l\in\mathcal{L}_c\cup\{0\}} y_{vcl}s_{cv}(l)$ where $c = c_{|\mathcal{C}_v|}^v$ for all $v \in \mathcal{V}$, along with the rest of the constraints in (14)*, and change the objective function to the following:*

$$\min_{(x_{cl},y_{cvl},z)} \Big[w_d \sum_{c\in\mathcal{C}}\sum_{l\in\mathcal{L}_c} d_c(l)x_{cl} + w_i \sum_{c\in\mathcal{C}}\sum_{l\in\mathcal{L}_c} i_c(l)x_{cl} + w_r z\Big] \tag{15}$$

4.3 "Best-of" model in (5)

For each vulnerability $v \in \mathcal{V}$ define the set of (flow-based) positive auxiliary variables $y_{v,c,l} \geq 0$ for each $c \in \{0\} \cup \mathcal{C}_v$ and $l \in \mathcal{L}_c$, that is, a flow is considered for each control that affects vulnerability v, along with a "no-control" flow $y_{v,0,0}$. For each $v \in \mathcal{V}$, we impose the total "in-flow" corresponding to vulnerability v to be one, i.e., $\sum_{c\in\{0\}\cup\mathcal{C}_v, l\in\mathcal{L}_c} y_{v,c,l} = 1$. We will also impose the logical "selection" constraints: $y_{v,c,l} \leq x_{cl}$ such that, if a control is not implemented, the corresponding flows will be zero. Then, in (5), we can simply replace $S_v(\boldsymbol{x}) = \min_{c\in\mathcal{C}_v} s_{cv}(x_c)$ with $\sum_{c\in\{0\}\cup\mathcal{C}_v, l\in\mathcal{L}_c} y_{v,c,l} s_{cv}(l)$, where we also define $s_{0v}(0) = 1$ as coefficients of $y_{v,0,0}$. To see that this conversion indeed works, note that when the total sum of the positive flow variables are constant, the minimization problem, trying to minimize the "out-flow" per each vulnerability, chooses the "pathway" with the highest available reduction, i.e. lowest flow coefficient, exactly as the "best-of" model intends. Putting together:

Prop. 5 *Each of the scalarized single objective optimizations in* (9) *for the best-of–passive risk model is equivalent to the following MILP:*

$$\min_{(x_{cl}, y_{cvl})} \Big[w_d \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} d_c(l) x_{cl} + w_i \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} i_c(l) x_{cl} + w_r \sum_{v\in\mathcal{V}} P_v \lambda_v \sum_{\substack{c\in\mathcal{C}_v\cup\{0\} \\ l\in\mathcal{L}_c}} y_{vcl} s_{cv}(l) \Big]$$

$$\textit{s. t.:} \quad \sum_{c\in\mathcal{C}} \sum_{l\in\mathcal{L}_c} d_c(l) x_{cl} \leq B, \quad \Big(0 \leq y_{vcl} \leq x_{cl},\ \forall v \in \mathcal{V}, \forall c \in \mathcal{C}_v, \forall l \in \mathcal{L}_c \Big),$$

$$\Big(\sum_{\substack{c\in\mathcal{C}_v\cup\{0\} \\ l\in\mathcal{L}_c}} y_{vcl} = 1,\ \forall v \in \mathcal{V} \Big), \quad \Big(\sum_{l\in\mathcal{L}_c} x_{cl} \leq 1,\ \forall c \in \mathcal{C} \Big), \quad \big(x_{cl} \in \{0,1\},\ \forall l \in \mathcal{L}_c, \forall c \in \mathcal{C} \big).$$

For the "reactive" threat model, the only difference is that the security risk (the third summation in the objective function) is replaced with the extra auxiliary (real-valued) variable z that needs to satisfy the following (linear) constraints: $z \geq \lambda_v \sum_{c\in\mathcal{C}_v\cup\{0\}, l\in\mathcal{L}_c} y_{vcl} s_{cv}(l),\ \forall v \in \mathcal{V}$.

5 From Vulnerabilities to Attacks

The expected losses (λ's) are more accurately related to attacks as opposed to vulnerabilities. For instance, consider an attack A whose success requires successful exploitation of two vulnerabilities v_1 and v_2, as part of the stages of the attack, and if successful inflicts an expected damage of λ_A. Since λ_A is only inflicted when both vulnerabilities are successfully exploited, it is not possible to separate the expected loss among v_1 and v_2 separately. We provide two different models for considering attacks that involve exploiting multiple vulnerabilities and describe how our developed MILPs can be extended to them.

5.1 Independence across vulnerabilities

Let $\mathcal{A}$ represent the set of attacks, where the expected inflicted loss if attack $A \in \mathcal{A}$ is successful is λ_A. Consider the multiplicative model in which the effect of

controls on a vulnerability was assumed to be independent. Now assume further that the successful exploitation of different vulnerabilities comprising an attack are also independent events. Then, the expected security damages will be:

$$R(\boldsymbol{x}) = \sum_{A \in \mathcal{A}} P_A \lambda_A \prod_{v \in A} \prod_{c \in \mathcal{C}_v} s_{cv}(x_c) = \sum_{A \in \mathcal{A}} P_A \lambda_A \prod_{c \in \mathcal{C}_v} \prod_{v \in A} s_{cv}(x_c)$$

This shows that, by introducing flow variables y_{Acl} for each attack, and performing a pre-processing by computing $s_{cA}(x_c) := \prod_{v \in A} s_{cv}(x_c)$, the same formulation as in Prep.4 can be applied with $s_{cv}(l)$ replaced by $s_{cA}(l)$.

5.2 Correlations across vulnerabilities

The success of exploitation attempts across different vulnerabilities comprising an attack may have positive correlations. These correlations arise due to skills or resources of the attackers: a successful exploitation of an stage of an attack can be a signal about the higher abilities/resources of the attacker. A model that reflects these correlations is the following: the success chance of carrying out an attack is determined by the lowest probability of success across the vulnerabilities that comprise that attack. Now, combining this model with the "best-of" model that takes the correlations across defensive mechanism of controls, we get:

$$R(\boldsymbol{x}) = \sum_{A \in \mathcal{A}} P_A \lambda_A \min_{v \in A} \min_{c \in \mathcal{C}_v} s_{cv}(x_c) = \sum_{A \in \mathcal{A}} P_A \lambda_A \min_{c \in \mathcal{C}_v} \min_{v \in A} s_{cv}(x_c)$$

Therefore, by introducing auxiliary variables y_{Acl} per attacks $A \in \mathcal{A}$ as opposed to per vulnerabilities, and performing a pre-processing $s_{cA}(l) := \min_{v \in A} s_{cv}(l)$, we can apply the same formulation as in Prop.5 with $s_{cv}(l)$ replaced by $s_{cA}(l)$.

6 Parameter Uncertainties

The most likely source of uncertainty in the parameters of our models is arguably the effectiveness of the controls against each of the vulnerabilities at different implementation levels, i.e., $e_{cv}(l)$'s. Suppose that each of these parameters are given as an uncertainty interval $[\underline{e}_{cv}(l), \overline{e}_{cv}(l)]$ a subset of $[0, 1]$, with the interpretation that the true (realized) value of the parameter can be anywhere in that interval with an unknown distribution. Collating all the efficacy parameters as $[\boldsymbol{e}_{cv}]$, we can show the uncertainty intervals by their lower and upper end in a concise way as: $[\underline{\boldsymbol{e}}_{cv}] \preceq [\boldsymbol{e}_{cv}] \preceq [\overline{\boldsymbol{e}}_{cv}]$, where $\preceq$ denotes element-wise inequalities.

One way to deal with the uncertainty is to optimize for the "worst" combined realization of the uncertain parameters. Consider the optimizations in (9), with the uncertain parameters $[\boldsymbol{e}_{cv}]$ also as variables. Then finding optimal plans with respect to worst case of the uncertainties in efficacies can be expressed as follows:

$$\begin{aligned} &\min_{\boldsymbol{x} \in \mathcal{X}} \left[\max_{[\underline{\boldsymbol{e}}_{cv}] \preceq [\boldsymbol{e}_{cv}] \preceq [\overline{\boldsymbol{e}}_{cv}]} \left\{ w_d \tilde{D}(\boldsymbol{x}) + w_i \tilde{I}(\boldsymbol{x}) + w_r \tilde{R}(\boldsymbol{x}, [\boldsymbol{e}_{cv}]) \right\} \right] \\ &\text{s.t.:} \max_{[\underline{\boldsymbol{e}}_{cv}] \preceq [e_{cv}] \preceq [\overline{\boldsymbol{e}}_{cv}]} \{ D(\boldsymbol{x}) - B \} \leq 0 \end{aligned} \tag{16}$$

We have the following observation, which we skip the proof of for brevity: For all of the security risk models in this paper, (16) is equivalent to:

$$\min_{\boldsymbol{x}\in\mathcal{X}} \left[w_d \tilde{D}(\boldsymbol{x}) + w_i \tilde{I}(\boldsymbol{x}) + w_r \tilde{R}(\boldsymbol{x}, [\underline{\boldsymbol{e}}_{cv}]) \right] \qquad \text{s.t.: } D(\boldsymbol{x}) \leq B$$

7 Numerical Evaluations

In this section, we first use our frameworks to investigate a list of the most important security controls for a typical SME (Small and Medium Enterprise) given a realistic set of parameters. As a soft method of validation, we compare the controls that most consistently appear in the Pareto-optimal plans against the top critical cyber-security controls as recommended by experts and policy organizations, specifically, SANS [17] and GCHQ [4,5]. Subsequently, we provide some comparisons among the different security models.[7]

Parameters for our Case Study: The vulnerabilities that a typical SME faces can be generally categorized into three groups: I. "Software Vulnerabilities", II. "Social Engineering" (e.g. phishing, pretexting, baiting, etc) and III. "Network Vulnerabilities". In this study, we incorporated a wide range of vulnerabilities from each of these categories. In total, we consider 37 most common vulnerabilities (Table I in the Appendix of our technical report [9]) which we collected from a combination of the publicly available databases such as the Critical Weakness Enumeration (CWE) and the Common Attack Pattern Enumeration and Classification (CAPEC).

Recall that the "Impact" score for each vulnerability in our models, i.e., I_v, designated the expected damage inflicted on the SME in case of a successful exploitation of that vulnerability. To obtain relative values for I_v, from the vulnerability descriptions in the "Common Weakness Scoring System (CWSS)", we derived a score for the impact of each vulnerability on three sources of damage: (1) "Data Losses", damages as a result of a compromise in the confidentiality or integrity of data; (2) "Business Disruption", losses due to compromise in the availability of services, and (3) "Reputation Damage". For each vulnerability, we considered a weighted average of these three damages as its overall impact. We estimated these by combining some relevant features from the Common Weakness Scoring System (CWSS) database. Specifically, features regarding their "System Requirement Score" (e.g. "required privilege"), "Technical Requirement Score" (e.g. "likelihood of discovery" and "ease of execution"), and "Environmental Factor Score" (e.g. "exploitability" and "accessibility of information"), are combined to give a measure of the "relative ease" to exploit each vulnerability and hence get a measure of the overall rate of attempts on each vulnerability. The general trend was similar to the measurement reports of [14].

For cyber-security controls, we need to have each control to be an actionable process as a single independent measure that can be used to help mitigate

[7] Due to space limit, some of our numerical evaluations were relegated to our technical report, accessible at: [9].

vulnerabilities in the system. We derived our controls from the "SANS Top 20 Critical Security controls", but we separated some of the controls that were in fact represented a composition of multiple investment decisions. Therefore, overall, we take into account 27 distinct controls, each with multiple levels of implementation, leading to 75 distinct controls. We estimated and normalized costs parameters (both indirect and indirect costs) reported in Table II in the Appendix of our technical report [9]. We also gathered estimates of the efficacy parameters based on the defensive mechanism of each measure in the face of the exploitation requirements of each vulnerability (Table III in the Appendix of our technical report [9]).

Validation Our overall objective is to provide a cyber-security investment framework which is accurate, credible and relevant to the real world. A rigorous validation should take the form of a field validation in the style of clinical trials. However, at this stage, for both economical and security reasons, this approach is not feasible. In reflecting about what can constitute a reasonable validation of our framework we have decided to concentrate on expert advice, in particular the available recommendations from government agencies. These agencies have studied thousands of cyber-security incidents over many years and as such we consider their advice credible and relevant. In particular, we consult with the SANS institute "The Critical Security Controls for Effective Cyber Defense" [17], and the "10 Steps to Cyber Security" [5] and "Common Cyber Attacks: Reducing The Impact" by GCHQ [4].

A subset of the critical controls is common among all of these documents. For instance from the SANS institute the core of recommended controls are the "5 quick wins" [17]: I- Application whitelisting (found in CSC-2); II- Use of standard, secure system configurations (found in CSC-3); III- Patching application software within 48 hours (found in CSC-4); IV- Patching system software within 48 hours (found in CSC 4); and V- Reducing the number of users with administrative privileges (found in CSC 3 and CSC 12)". A similar set of critical controls is recommended by the latest GCHQ advice [4]: I- Boundary firewalls and Internet gateways; II- Malware protection; III- Patch management; IV- Whitelisting and execution control; V- Secure configuration; VI- Password policy; VII- User access control; It is hence interesting to compare our results with these sets of recommendations and in particular their intersection: I- Patch management; II- Application whitelisting; III- Secure configuration; IV- User access control.

To make a meaningful comparison we have organized the controls appearing in our solutions in a "prevalence ordering". The "most prevalent" controls are the ones that appear across the most number of Pareto-optimal plans for a large range of parameters: we take this as a measure of the relative importance of each cyber-security control. In particular, For each of our models, we computed the number of times each cyber-security control (at any of its implementation levels) appear in the plan across all Pareto-optimal solutions. We then "ranked" the controls based on this measure of prevalence in decreasing order. The resulting ranks are provided in Table 1 in the Appendix. We observed that overall, "patching", "firewalls" and "whitelisting" appear among the top controls for

all cases and there is a general consistency with the official recommendations. The best match with the official recommendations pertains to the "Best-of – Reactive" model. This reinforces the intuition that the "Best-of" combination of controls concentrates on the contributions of the most effective controls, and the "Reactive" threat concentrates on the most critical vulnerabilities. This observation also underlines the importance of taking into account the hitherto ignored correlations in the defensive mechanisms of the security controls.

The consistency of our results and the official advice is an encouraging first step. In the longer term we expect our mathematical framework to guide and eventually possibly replace expert advice. Another advantage is that we can customize our data to specific organizations and particular threats and so provide better "individualized" investment portfolios than a generic one-size-fit-all recommendation. We can also extend and edit the data with new controls and attacks as the threat scenarios evolve. Our solutions can be efficiently computed for large sets of controls and attacks, way beyond human manual capabilities. Our framework and the resulting tools hence open the door for customizable and accurate quantitative cyber-security advice.

A note on the computational efficiency of our frameworks It is worth noting that, with their distinct implementation levels, we are considering 75 distinct security controls, which lead to an order of 10^{14} distinct cyber-security plans. With this size of the problem, an exhaustive search for finding Pareto-optimal plans is outright impractical. Generic heuristic methods such as "Genetic Algorithms" and "Tabu Search" as used in works like [13,24] will also take "days" to converge, and even after convergence, there is no guarantee of optimality. In contrast, our MILP-based frameworks, using a generic MILP solver (Matlab's `intlinprog` in our case on a typical laptop) solve for an "exact" optimal solution over the following time scales: "additive" (both passive and reactive): fraction of a second; "Multiplicative" (both "passive" and "reactive"): less than a minute; and surprisingly, for "Best-of" model, about a second for the "passive" case, and less than 10 seconds for the reactive case.

Conclusions and future works

Decision support for cyber-security is a complex multi-objective problem. We modeled a large set of possible vulnerabilities and mitigations, and demonstrated how to efficiently compute Pareto-optimal solutions using Mixed Integer Linear Programming conversions. Many challenges remain, e.g. taking into account the costs of attacks, custom combined efficacies of controls, other approaches to deal with parameter uncertainties, combining learning and optimization, and stronger model validation. Some of these problems are within the realm of optimization engineering, others like validation methodologies requires more real-world data, which will be direction of our future work.

8 Acknowledgment

The research for this paper was supported by EPSRC project EP/K005820/1 "Games and Abstraction: The Science of Cyber Security".

References

1. Anderson, R., Moore, T.: The economics of information security. Science 314(5799) (2006)
2. Butler, S.A.: Security attribute evaluation method: a cost-benefit approach. In: Proc. of the 24th international conference on Software engineering. ACM (2002)
3. Cavusoglu, H., Raghunathan, S., Yue, W.T.: Decision-theoretic and game-theoretic approaches to it security investment. Journal of Management Information Systems 25(2) (2008)
4. CESG: Common cyber attacks: Reducing the impact. `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf`, web. 2016-04-13
5. CESG (UK's Nat. Tech. Authority for Inf. Assurance): 10 Steps to Cyber Security. `https://www.cesg.gov.uk/10-steps-cyber-security`, web. 2016-04-13
6. Chinchuluun, A., Pardalos, P.M.: A survey of recent developments in multiobjective optimization. Annals of Operations Research 154(1) (2007)
7. Dewri, R., Poolsappasit, N., Ray, I., Whitley, D.: Optimal security hardening using multi-objective optimization on attack tree models of networks. In: Proc. of the 14th ACM conference on Computer and communications security. ACM (2007)
8. Gupta, M., Rees, J., Chaturvedi, A., Chi, J.: Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. Decision Support Systems 41(3) (2006)
9. Khouzani, M., Malacaria, P., Hankin, C., Fielder, A., Smeraldi, F.: Efficient numerical frameworks for multi-objective cyber security planning: Tech. report. `http://www.eecs.qmul.ac.uk/~khouzani/Papers/ESORICS16Techrep.pdf`, web.
10. Marler, R.T., Arora, J.S.: Survey of multi-objective optimization methods for engineering. Structural and multidisciplinary optimization 26(6) (2004)
11. Nagurney, A., Nagurney, L.S., Shukla, S.: A supply chain game theory framework for cybersecurity investments under network vulnerability. In: Computation, Cryptography, and Network Security. Springer (2015)
12. Ojamaa, A., Tyugu, E., Kivimaa, J.: Pareto-optimal situaton analysis for selection of security measures. In: Military Communications Conference. IEEE (2008)
13. Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., Smeraldi, F.: Cybersecurity games and investments: a decision support approach. In: Decision and Game Theory for Security. Springer (2014)
14. Passeri, P.: HACKMAGEDDON, information security timelines and statistics. `http://www.hackmageddon.com`, web. 2016-04-19
15. Poolsappasit, N., Dewri, R., Ray, I.: Dynamic security risk management using bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing 9(1) (2012)
16. Rees, L.P., Deane, J.K., Rakes, T.R., Baker, W.H.: Decision support for cybersecurity risk planning. Decision Support Systems 51(3) (2011)
17. SANS: The critical security controls for effective cyber defense. `https://www.sans.org/media/critical-security-controls/CSC-5.pdf`, web. 2016-04-13

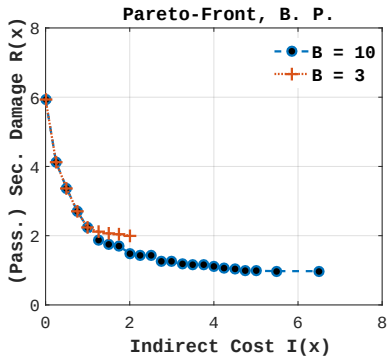
18. Sarala, R., Zayaraz, G., Vijayalakshmi, V.: Optimal selection of security countermeasures for effective information security. In: Proc. of the International Conference on Soft Computing Systems. Springer (2016)
19. Sawik, T.: Selection of optimal countermeasure portfolio in it security planning. Decision Support Systems 55(1) (2013)
20. Schechter, S.E.: Computer Security Strength & Risk: A Quantitative Approach. Ph.D. thesis, Harvard University Cambridge, Massachusetts (2004)
21. Syalim, A., Hori, Y., Sakurai, K.: Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide. In: International Conference on Availability, Reliability and Security. IEEE (2009)
22. UK's Department for Business, Innovation & Skills: Cyber Essentials Scheme. `https://www.gov.uk/government/publications/cyber-essentials-scheme-overview`, web. 2016-01-07
23. Ulungu, E.L., Teghem, J.: Multi-objective combinatorial optimization problems: A survey. Journal of Multi-Criteria Decision Analysis 3(2) (1994)
24. Viduto, V., Maple, C., Huang, W., López-Peréz, D.: A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. Decision Support Systems 53(3) (2012)

Appendix

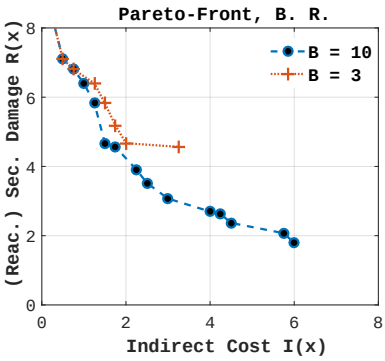
Table 1: Order of prevalence of controls among Pareto-optimal plans, for different security models. In the column-headers, the initials "A.", "M." and "B." stand for "Additive", "Multiplicative" and "Best-of", also, "P." and "R." designate "Reactive" and "Passive", respectively. The table is ordered with respect to the Best-of prevalence rank, as it shows the best match with expert recommendation.

Cyber-Security Control	B.R.	M.R.	A.R.	B.P.	M.P.	A.P.
Deployment of Network Firewalls	1	1	1	2	2	2
Deploy Web Application Firewalls	2	2	4	4	3	3
Anti-Malware Software	3	7	6	3	4	5
Automated Patching Tools	4	3	2	1	1	1
Use of Secure Config. for OS	5	5	7	5	10	9
Application Whitelisting	6	4	3	10	8	8
Network Data Encryption	7	6	5	7	6	4
Strong Secure Password Policy	8	15	20	13	12	17
User Access Controls	9	12	17	6	7	13
Secure Configuration Controls for All Devices	10	24	26	9	15	22
Penetration Testing	11	13	13	27	27	12
Automated Vulnerability Scanning Tools	12	11	11	17	13	18
Automated Inventory Scanning & Management	13	8	8	16	14	11
Segmentation of Network Based on Trust Levels	14	17	22	23	23	19
Host Based IPS	15	9	16	12	5	7
Deploy DLP Based Systems	16	22	24	8	16	25
Execution Control on Removable Media	17	21	15	18	17	21
Employ Wireless Devices Authentication Config.	18	23	25	19	18	26
Employ Port Scanning & Control Tools	19	25	21	20	19	23
Deploy Network Based IDS	20	20	19	14	20	20
Deploy Network Based Proxies	21	16	14	21	21	14
Deployment of VLANs for Sensitive Operations	22	26	27	22	22	27
Website Whitelisting	23	27	18	11	11	16
Network Log Reporting	24	14	12	24	24	10
Account Management Controls	25	19	23	25	25	24
User Training & Education	26	18	10	26	26	15
Incident Handling & Response Policies	27	10	9	15	9	6

Further Numerical Investigations: Choosing an optimal plan from the Pareto-front



(a) Passive Threat



(b) Reactive Threat

Fig. 1: Examples of Pareto-front plots. The efficacy combination model is "best-of", and the threat model is "passive" in (a) and "reactive" in (b).

Table I: Vulnerabilities.

ID	Vulnerability (v)	I_v	P_v	$P_v I_v$
V1	OS Command Injection	5.9	0.027	0.16
V2	XSS	5.9	0.032	0.19
V3	SQL Injection	4.4	0.030	0.13
V4	Error Message Exposure	3.0	0.010	0.03
V5	Cross Site Request Forgery	8.3	0.031	0.25
V6	Race Condition	3.0	0.014	0.04
V7	Unrestricted Upload	4.0	0.015	0.06
V8	Open Redirect	5.4	0.028	0.15
V9	Path Traversal	5.4	0.019	0.10
V10	Improper Control of Filenames	4.7	0.020	0.09
V11	Buffer Overflow	3.6	0.030	0.11
V12	Improper Validation of Array Indices	3.6	0.028	0.10
V13	Unrestricted Allocation of Resources	3.6	0.038	0.14
V14	Integer Overflow or Wraparound	3.6	0.026	0.09
V15	Download of Code Without Integrity Checks	6.4	0.025	0.16
V16	Improper Check for Unusual or Exceptional Conditions	4.4	0.021	0.09
V17	Improper Authorisation	7.1	0.026	0.18
V18	Missing Authentication for Critical Factors	7.1	0.031	0.22
V19	Missing Encryption on Sensitive Data	7.1	0.029	0.20
V20	Risky or Broken Cryptographic Algorithms	4.1	0.016	0.06
V21	Incorrect Permission Assignment for Critical Resources	6.0	0.020	0.12
V22	Use of Hard Coded Credentials	4.7	0.039	0.18
V23	Spear Phishing (Credentials)	8.3	0.029	0.24
V24	Spear Phishing (Malware)	8.4	0.029	0.25
V25	Pretexting (Credentials)	8.3	0.029	0.24
V26	Phishing (Credentials)	8.3	0.033	0.27
V27	Phishing (Malware)	8.4	0.033	0.27
V28	Watering Hole (Malware)	8.4	0.032	0.27
V29	Baiting (Malware)	8.4	0.032	0.27
V30	DDoS	3.0	0.037	0.11
V31	Port Scanning Attacks	6.6	0.041	0.27
V32	Unauthorised Direct Access	6.6	0.041	0.27
V33	IP Spoofing Attacks	6.8	0.032	0.22
V34	Unsecured Third Party Software	6.4	0.006	0.04
V35	Infected BYOD	7.4	0.016	0.12
V36	Passive Monitoring	3.0	0.034	0.10
V37	Session Hijacking	4.8	0.020	0.10

Control Costs (direct and indirect) ... [continued on the next page]

ID	Control(c)	Level(l)	d_c	I_c
C1-1	Automated Inventory Scanning & Management	Implement Once	0.25	0.25
C1-2	Automated Inventory Scanning & Management	Yearly	0.50	0.25
C1-3	Automated Inventory Scanning & Management	Monthly	0.75	0.50
C1-4	Automated Inventory Scanning & Management	Weekly	1.00	0.50
C1-5	Automated Inventory Scanning & Management	Daily/On Demand	1.50	0.75
C2-1	Automated Patching Tools	Implement Once	0.25	0.25
C2-2	Automated Patching Tools	Yearly	0.50	0.25
C2-3	Automated Patching Tools	Monthly	0.75	0.50
C2-4	Automated Patching Tools	Weekly	1.00	0.75
C2-5	Automated Patching Tools	Daily/On Demand	1.50	0.25
C3-1	Automated Vulnerability Scanning Tools	Yearly	0.50	0.25
C3-2	Automated Vulnerability Scanning Tools	Monthly	0.75	0.50
C3-3	Automated Vulnerability Scanning Tools	Weekly	1.00	0.75
C3-4	Automated Vulnerability Scanning Tools	Daily/On Demand	1.50	0.25
C4-1	Anti-Malware Software	Yearly	0.50	0.25
C4-2	Anti-Malware Software	Monthly	0.75	0.50
C4-3	Anti-Malware Software	Weekly	1.00	0.75
C4-4	Anti-Malware Software	Daily/On Demand	1.50	1.25
C5-1	Deployment of Network Firewalls	Lax	0.25	0.25
C5-2	Deployment of Network Firewalls	Moderate	0.50	0.50
C5-3	Deployment of Network Firewalls	Strict	1.00	0.50
C6-1	Host Based IPS	Lax	0.75	0.25
C6-2	Host Based IPS	Moderate	1.00	0.50
C6-3	Host Based IPS	Strict	1.50	0.75
C7-1	Deploy Web Application Firewalls	Lax	0.25	0.25
C7-2	Deploy Web Application Firewalls	Moderate	0.50	0.50
C7-3	Deploy Web Application Firewalls	Strict	1.00	0.50
C8-1	Deploy DLP Based Systems	Implement Once	1.00	0.25
C9-1	Use of Secure Config for OS	Basic	1.00	0.25
C9-2	Use of Secure Config for OS	Advanced	1.25	0.50
C9-3	Use of Secure Config for OS	Complete	1.50	0.75
C10-1	Execution Control on Removable Media	Lax	0.25	0.75
C10-2	Execution Control on Removable Media	Moderate	0.50	1.25
C10-3	Execution Control on Removable Media	Strict	0.75	1.75
C11-1	Employ Wireless Devices Auth. Config	Implement Once	1.00	0.75
C12-1	Secure Configuration Controls for All Devices	Basic	1.00	1.25
C12-2	Secure Configuration Controls for All Devices	Advanced	1.25	1.50
C12-3	Secure Configuration Controls for All Devices	Complete	1.50	2.00
C13-1	Employ Port Scanning & Control Tools	Yearly	0.25	0.25
C13-2	Employ Port Scanning & Control Tools	Monthly	0.50	0.50
C13-3	Employ Port Scanning & Control Tools	Weekly	1.00	0.50
C13-4	Employ Port Scanning & Control Tools	Daily/On Demand	1.50	0.75
C14-1	Deploy Network Based IDS	Basic	0.75	0.25
C14-2	Deploy Network Based IDS	Advanced	1.00	0.50
C14-3	Deploy Network Based IDS	Complete	1.25	0.75
C15-1	Deploy Network Based Proxies	Implement Once	1.00	0.50
C16-1	Deployment of VLANs for Sensitive Operations	Implement Once	1.25	0.50
C17-1	Segmentation of Net. Based on Trust Levels	Implement Once	2.00	0.50
C18-1	Network Data Encryption	Implement Once	0.75	0.75
C19-1	Application Whitelisting	Lax	0.50	0.75
C19-2	Application Whitelisting	Moderate	1.00	1.25
C19-3	Application Whitelisting	Strict	1.25	1.50
C19-4	Application Whitelisting	Business Needs	1.50	1.75

Table II: Control Costs (direct and indirect) ... [continue from previous page]

ID	Control(c)	Level(l)	d_c	I_c
C20-1	User Access Controls	Basic	0.50	0.75
C20-2	User Access Controls	Advanced	1.00	1.00
C20-3	User Access Controls	Complete	2.00	1.50
C21-1	Website Whitelisting	Lax	0.50	0.75
C21-2	Website Whitelisting	Moderate	1.00	1.25
C21-3	Website Whitelisting	Strict	1.25	1.50
C21-4	Website Whitelisting	Business Needs	1.50	2.25
C22-1	Network Log Reporting	Implement Once	0.75	0.25
C23-1	Account Management Controls	Lax	0.75	0.75
C23-2	Account Management Controls	Moderate	1.00	1.00
C23-3	Account Management Controls	Strict	1.50	1.00
C23-4	Account Management Controls	Business Needs	1.75	1.50
C24-1	User Training & Education	Yearly	0.75	0.50
C24-2	User Training & Education	Monthly	1.00	1.00
C24-3	User Training & Education	Weekly	2.00	1.50
C24-4	User Training & Education	Daily/On Demand	4.00	2.00
C25-1	Strong Secure Password Policy	Lax	0.25	0.50
C25-2	Strong Secure Password Policy	Moderate	1.00	0.75
C25-3	Strong Secure Password Policy	Strict	1.50	1.25
C26-1	Incident Handling & Response Policies	Implement Once	0.25	0.50
C27-1	Penetration Testing	Yearly	2.00	0.25
C27-2	Penetration Testing	Monthly	4.00	0.50

Table III: Control-Vulnerability Effectiveness: $ecv(l)$...[continues on next page]

ID	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19
C1-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C1-2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C1-3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C1-4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C1-5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C2-1	0.09	0.09	0.09	0.18	0.09	0.18	0.09	0.45	0.45	0.45	0.18	0.18	0.18	0.18	0.09	0.18	0.18	0.18	-
C2-2	0.23	0.18	0.45	0.45	0.18	0.23	0.18	0.45	0.45	0.45	0.27	0.27	0.27	0.27	0.18	0.23	0.23	0.23	-
C2-3	0.54	0.27	0.63	0.63	0.27	0.54	0.27	0.85	0.85	0.85	0.45	0.45	0.45	0.45	0.27	0.54	0.54	0.54	-
C2-4	0.68	0.36	0.85	0.85	0.36	0.68	0.36	0.85	0.85	0.85	0.68	0.68	0.68	0.68	0.36	0.63	0.63	0.63	-
C2-5	0.85	0.45	0.85	0.85	0.45	0.85	0.45	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.45	0.68	0.68	0.68	-
C3-1	0.09	0.09	-	-	0.09	0.09	-	0.45	0.45	0.45	0.27	0.27	0.27	0.27	-	0.09	0.09	0.09	-
C3-2	0.27	0.18	-	-	0.18	0.27	-	0.85	0.85	0.85	0.45	0.45	0.45	0.45	-	0.18	0.18	0.18	-
C3-3	0.54	0.27	-	-	0.27	0.54	-	0.85	0.85	0.85	0.68	0.68	0.68	0.68	-	0.27	0.27	0.27	-
C3-4	0.68	0.45	-	-	0.45	0.68	-	0.85	0.85	0.85	0.85	0.85	0.85	0.85	-	0.27	0.27	0.27	-
C4-1	-	-	-	-	-	-	0.18	-	-	-	-	-	-	-	0.18	-	-	-	-
C4-2	-	-	-	-	-	-	0.45	-	-	-	-	-	-	-	0.45	-	-	-	-
C4-3	-	-	-	-	-	-	0.54	-	-	-	-	-	-	-	0.54	-	-	-	-
C4-4	-	-	-	-	-	-	0.68	-	-	-	-	-	-	-	0.68	-	-	-	-
C5-1	0.09	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C5-2	0.27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C5-3	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C6-1	0.09	-	-	-	-	-	-	0.09	0.09	0.09	0.09	0.09	0.09	0.09	-	0.27	0.27	0.27	-
C6-2	0.27	-	-	-	-	-	-	0.27	0.27	0.27	0.27	0.27	0.27	0.27	-	0.45	0.45	0.45	-
C6-3	0.45	-	-	-	-	-	-	0.45	0.45	0.45	0.45	0.45	0.45	0.45	-	0.63	0.63	0.63	-
C7-1	-	0.18	-	-	0.18	-	0.09	-	-	-	-	-	-	-	0.09	-	-	-	-
C7-2	-	0.45	-	-	0.45	-	0.18	-	-	-	-	-	-	-	0.18	-	-	-	-
C7-3	-	0.85	-	-	0.85	-	0.27	-	-	-	-	-	-	-	0.27	-	-	-	-
C8-1	-	-	0.45	0.09	-	0.27	-	-	-	-	-	-	-	-	-	0.45	0.45	0.45	-
C9-1	0.32	-	-	0.45	-	0.32	-	0.45	0.45	0.45	0.09	0.09	0.09	0.09	-	0.27	0.27	0.27	0.45
C9-2	0.45	-	-	0.58	-	0.45	-	0.63	0.63	0.63	0.27	0.27	0.27	0.27	-	0.63	0.63	0.63	0.63
C9-3	0.68	-	-	0.68	-	0.68	-	0.85	0.85	0.85	0.45	0.45	0.45	0.45	-	0.85	0.85	0.85	0.85
C10-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C10-2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C10-3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C11-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C12-1	0.32	-	-	0.45	-	0.32	-	-	-	-	0.32	0.32	0.32	0.32	-	0.27	0.27	0.27	0.45
C12-2	0.45	-	-	0.58	-	0.45	-	-	-	-	0.45	0.45	0.45	0.45	-	0.63	0.63	0.63	0.63
C12-3	0.68	-	-	0.68	-	0.68	-	-	-	-	0.58	0.58	0.58	0.58	-	0.85	0.85	0.85	0.85
C13-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C13-2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C13-3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C13-4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C14-1	0.09	-	0.18	-	-	-	-	0.18	0.18	0.18	0.09	0.09	0.09	0.09	-	0.09	0.09	0.09	-
C14-2	0.27	-	0.36	-	-	-	-	0.36	0.36	0.36	0.27	0.27	0.27	0.27	-	0.27	0.27	0.27	-
C14-3	0.45	-	0.54	-	-	-	-	0.54	0.54	0.54	0.45	0.45	0.45	0.45	-	0.45	0.45	0.45	-
C15-1	0.18	-	-	-	-	-	-	0.45	0.45	0.45	-	-	-	-	-	-	-	-	-
C16-1	0.27	-	0.45	-	-	-	0.45	-	-	-	-	-	-	-	0.45	-	-	-	-
C17-1	0.23	-	-	-	-	-	0.23	-	-	-	-	-	-	-	0.23	0.27	0.27	0.27	-
C18-1	-	-	-	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.85
C19-1	-	-	-	0.09	-	0.09	0.18	0.18	0.18	0.18	0.09	0.09	0.09	0.09	0.18	0.09	0.09	0.09	-
C19-2	-	-	-	0.27	-	0.27	0.36	0.36	0.36	0.36	0.54	0.54	0.54	0.54	0.45	0.27	0.27	0.27	-
C19-3	-	-	-	0.45	-	0.45	0.54	0.54	0.54	0.54	0.63	0.63	0.63	0.63	0.63	0.45	0.45	0.45	-
C19-4	-	-	-	0.54	-	0.54	0.72	0.72	0.72	0.72	0.72	0.72	0.72	0.72	0.72	0.54	0.54	0.54	-
C20-1	0.09	-	-	0.18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C20-2	0.27	-	-	0.32	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C20-3	0.45	-	-	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C21-1	-	0.18	-	-	0.18	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C21-2	-	0.45	-	-	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C21-3	-	0.63	-	-	0.63	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C21-4	-	0.85	-	-	0.85	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C22-1	0.18	-	0.18	-	-	0.27	-	-	-	-	-	-	-	-	-	-	-	-	-
C23-1	-	-	0.09	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C23-2	-	-	0.27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C23-3	-	-	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C23-4	-	-	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C24-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C24-2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C24-3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C24-4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C25-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C25-2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C25-3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C26-1	0.09	-	0.09	-	-	0.09	-	-	-	-	-	-	-	-	-	-	-	-	-
C27-1	0.18	-	0.18	-	-	0.36	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18
C27-2	0.27	-	0.36	-	-	0.45	0.27	0.27	0.27	0.27	0.27	0.27	0.27	0.27	0.27	0.27	0.27	0.27	0.27

Table III: Control-Vulnerability Effectiveness: $ecv(l)$...[from previous page]

	V20	V21	V22	V23	V24	V25	V26	V27	V28	V29	V30	V31	V32	V33	V34	V35	V36	V37
C1-1	-	-	-	0.09	-	0.09	0.09	-	-	-	-	0.18	0.18	0.18	-	0.09	-	-
C1-2	-	-	-	0.18	-	0.18	0.18	-	-	-	-	0.23	0.23	0.23	-	0.18	-	-
C1-3	-	-	-	0.27	-	0.27	0.27	-	-	-	-	0.45	0.45	0.45	-	0.27	-	-
C1-4	-	-	-	0.36	-	0.36	0.36	-	-	-	-	0.54	0.54	0.54	-	0.36	-	-
C1-5	-	-	-	0.45	-	0.45	0.45	-	-	-	-	0.63	0.63	0.63	-	0.45	-	-
C2-1	-	0.18	0.18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C2-2	-	0.23	0.23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C2-3	-	0.54	0.54	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C2-4	-	0.63	0.63	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C2-5	-	0.68	0.68	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C3-1	-	0.09	0.09	-	-	-	-	-	-	-	-	0.18	0.18	-	-	-	-	-
C3-2	-	0.18	0.18	-	-	-	-	-	-	-	-	0.45	0.45	-	-	-	-	-
C3-3	-	0.27	0.27	-	-	-	-	-	-	-	-	0.63	0.63	-	-	-	-	-
C3-4	-	0.27	0.27	-	-	-	-	-	-	-	-	0.68	0.68	-	-	-	-	-
C4-1	-	-	-	-	0.45	-	-	0.45	0.45	0.45	-	-	-	-	0.09	-	-	-
C4-2	-	-	-	-	0.63	-	-	0.63	0.63	0.63	-	-	-	-	0.27	-	-	-
C4-3	-	-	-	-	0.81	-	-	0.81	0.81	0.81	-	-	-	-	0.45	-	-	-
C4-4	-	-	-	-	0.85	-	-	0.85	0.85	0.85	-	-	-	-	0.63	-	-	-
C5-1	-	-	-	0.18	-	0.18	0.18	-	-	-	0.18	0.63	0.63	0.63	-	0.36	0.27	0.36
C5-2	-	-	-	0.45	-	0.45	0.45	-	-	-	0.36	0.81	0.81	0.81	-	0.54	0.36	0.54
C5-3	-	-	-	0.63	-	0.63	0.63	-	-	-	0.54	0.85	0.85	0.85	-	0.72	0.54	0.72
C6-1	-	0.27	0.27	0.18	-	0.18	0.18	-	-	-	-	0.63	0.63	0.63	-	-	0.27	0.27
C6-2	-	0.45	0.45	0.45	-	0.45	0.45	-	-	-	-	0.81	0.81	0.81	-	-	0.45	0.45
C6-3	-	0.63	0.63	0.63	-	0.63	0.63	-	-	-	-	0.85	0.85	0.85	-	-	0.63	0.63
C7-1	-	-	-	-	0.27	-	-	0.27	0.27	0.27	-	-	-	-	-	-	-	-
C7-2	-	-	-	-	0.45	-	-	0.45	0.45	0.45	-	-	-	-	-	-	-	-
C7-3	-	-	-	-	0.63	-	-	0.63	0.63	0.63	-	-	-	-	-	-	-	-
C8-1	-	0.45	0.45	-	-	-	-	-	-	-	-	-	-	-	-	-	0.63	0.63
C9-1	0.45	0.27	0.27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C9-2	0.63	0.63	0.63	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C9-3	0.85	0.85	0.85	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
C10-1	-	-	-	-	-	-	-	-	-	0.63	-	-	-	-	0.09	0.09	-	-
C10-2	-	-	-	-	-	-	-	-	-	0.72	-	-	-	-	0.27	0.27	-	-
C10-3	-	-	-	-	-	-	-	-	-	0.81	-	-	-	-	0.45	0.45	-	-
C11-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.81	-	-
C12-1	0.45	0.27	0.27	-	-	-	-	-	-	-	-	-	-	-	-	0.36	-	-
C12-2	0.63	0.63	0.63	-	-	-	-	-	-	-	-	-	-	-	-	0.54	-	-
C12-3	0.85	0.85	0.85	-	-	-	-	-	-	-	-	-	-	-	-	0.81	-	-
C13-1	-	-	-	-	-	-	-	-	-	-	-	0.45	0.45	0.45	-	-	-	-
C13-2	-	-	-	-	-	-	-	-	-	-	-	0.63	0.63	0.63	-	-	-	-
C13-3	-	-	-	-	-	-	-	-	-	-	-	0.81	0.81	0.81	-	-	-	-
C13-4	-	-	-	-	-	-	-	-	-	-	-	0.85	0.85	0.85	-	-	-	-
C14-1	-	0.09	0.09	0.09	-	0.09	0.09	-	-	-	-	-	-	-	-	-	0.36	0.36
C14-2	-	0.27	0.27	0.27	-	0.27	0.27	-	-	-	-	-	-	-	-	-	0.54	0.54
C14-3	-	0.45	0.45	0.45	-	0.45	0.45	-	-	-	-	-	-	-	-	-	0.72	0.72
C15-1	-	-	-	-	-	-	-	-	-	-	0.09	-	-	-	-	0.63	-	-
C16-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.81	-	-
C17-1	-	0.27	0.27	0.36	0.36	0.36	0.36	0.36	0.36	0.36	-	-	-	-	-	0.63	0.45	0.45
C18-1	0.85	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.63	0.63
C19-1	-	0.09	0.09	-	0.45	-	-	0.18	0.18	0.18	-	-	-	-	0.45	-	-	-
C19-2	-	0.27	0.27	-	0.63	-	-	0.36	0.36	0.36	-	-	-	-	0.63	-	-	-
C19-3	-	0.45	0.45	-	0.81	-	-	0.54	0.54	0.54	-	-	-	-	0.81	-	-	-
C19-4	-	0.54	0.54	-	0.85	-	-	0.63	0.63	0.63	-	-	-	-	0.85	-	-	-
C20-1	-	-	-	0.45	-	0.45	0.45	-	-	-	-	0.45	0.45	0.45	-	0.27	0.18	0.18
C20-2	-	-	-	0.68	-	0.68	0.68	-	-	-	-	0.63	0.63	0.63	-	0.54	0.36	0.36
C20-3	-	-	-	0.85	-	0.85	0.85	-	-	-	-	0.85	0.85	0.85	-	0.81	0.54	0.54
C21-1	-	-	-	0.18	0.45	0.18	0.18	0.18	0.45	0.45	-	-	-	-	-	-	-	-
C21-2	-	-	-	0.27	0.63	0.27	0.27	0.27	0.63	0.63	-	-	-	-	-	-	-	-
C21-3	-	-	-	0.45	0.81	0.45	0.45	0.45	0.81	0.81	-	-	-	-	-	-	-	-
C21-4	-	-	-	0.54	0.85	0.54	0.54	0.54	0.85	0.85	-	-	-	-	-	-	-	-
C22-1	-	-	-	-	-	-	-	-	-	-	0.09	-	-	-	-	0.27	-	-
C23-1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.18	-	0.27	0.27
C23-2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.36	-	0.45	0.45
C23-3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.54	-	0.63	0.63
C23-4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.81	-	0.63	0.63
C24-1	-	-	-	0.18	0.18	0.18	0.18	0.18	0.18	0.18	-	-	-	-	0.18	0.18	-	0.09
C24-2	-	-	-	0.27	0.27	0.27	0.27	0.27	0.27	0.27	-	-	-	-	0.27	0.27	-	0.18
C24-3	-	-	-	0.36	0.36	0.36	0.36	0.36	0.36	0.36	-	-	-	-	0.36	0.36	-	0.23
C24-4	-	-	-	0.45	0.45	0.45	0.45	0.45	0.45	0.45	-	-	-	-	0.45	0.45	-	0.27
C25-1	-	-	-	0.27	-	0.27	0.27	-	-	-	-	-	-	-	-	-	0.27	0.27
C25-2	-	-	-	0.54	-	0.54	0.54	-	-	-	-	-	-	-	-	-	0.45	0.45
C25-3	-	-	-	0.81	-	0.81	0.81	-	-	-	-	-	-	-	-	-	0.63	0.63
C26-1	-	-	-	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.09	-	-	-	-	-	-	-
C27-1	0.18	0.18	0.18	0.09	0.09	0.09	0.09	0.09	0.09	0.09	-	0.36	0.36	0.36	-	0.27	-	-
C27-2	0.27	0.27	0.27	0.09	0.09	0.09	0.09	0.09	0.09	0.09	-	0.36	0.36	0.36	-	0.36	-	-